PrivacyPillar

Privacy Laws, Untangled: Your Quick-Read Guide

Data is the new currency - and like any currency, it comes with rules, restrictions, and regulators keeping watch. Whether you're running a startup in Bangalore, scaling a SaaS in Berlin, or selling sneakers in San Francisco, privacy laws are no longer "someone else's problem." They're yours.
The challenge? Every region has its own playbook:

- India with the **Digital Personal Data Protection Act (DPDPA)**
- Europe with the heavyweight **GDPR**
- California leading the US front with the **CCPA**

All three share the same mission - protect people's personal data - but they differ in how they define, demand, and enforce compliance. And for businesses operating across borders, that can get complicated, fast.

This cheat sheet was designed to cut through the noise. It lays out the key obligations, rights and risks under each law side by side - so you can spot overlaps, spot differences, and know exactly where you need to tighten up your privacy game.

How to Use This Cheat Sheet

- **Compare at a glance:** Each section lines up DPDPA, GDPR, and CCPA on the same theme (consent, data rights, security, penalties, etc.).
- **Find your risk zones:** Identify where your current practices might fall short.
- **Plan for scale:** If you're expanding into new regions, this sheet shows you what extra boxes you'll need to tick.

Date of Publishing: September 2025

PrivacyPillar

Privacy Cheat Sheet

Topic	DPDPA & Draft Rules	GDPR	CCPA
Applicability	(Section 3) Applies to ■ Digital Personal Data processed in India ■ Digitised offline data ■ To overseas processing offering goods or services to individuals in India	(Article 3) Applies to ■ Personal data processing within the EU and of EU residents globally	(Section 1798.140) Applies to ■ Personal information of California residents collected by businesses
Data Types Covered	Digital Personal Data	Personal Data including special categorises (sensitive data) requiring extra protection	Personal information with specific sensitive categories defined (genetic data, financial data, race, etc.)
Children Data	(Section 9) ■ Parent/Guardian consent required for processing personal data of children ■ Restrictions for profiling and tracking children's data	(Article 8) ■ Consent required from parent/guardian for children under 16 (Member States may lower it to 13) ■ Special safeguards for children's data.tracking children's data	(Section 1798.120 (c)) ■ A business shall not sell the personal information of consumers if it has actual knowledge that the consumer is less than 16 years of age, unless: - For consumers aged 13 to less than 16: the consume has affirmatively authorised the sale (opt- in) - For consumers under 13: the consumer's parent or guardian has affirmatively authorised the sale (parental opt in)
Oversight Bodies	(Section 18) Data Protection Board of India (Regulatory and enforcement authority for DPDPA)	(Article 51-59) ■ Independent Supervisory Authority in each EU Member State ■ European Data Protection Board	(Section 1798.199) California Privacy Protection Agency
Consent	(Section 6) Consent must be free, specific, informed, unconditional and unambiguous with a clear affirmative action; exceptions for certain legitimate uses	(Article 4-7) ■ Consent must be freely given, specific, informed and unambiguous ■ Explicit consent to be taken in case of processing of Sensitive personal data	(Section-1798.120 - 1798.135) ■ No explicit general consent requirement ■ Consumers have opt-out rights for sale of personal data
Privacy Principles	(Section 4-8) ■ Purpose limitation ■ Data minimisation ■ Lawful processing ■ Accuracy of personal data ■ Storage limitation ■ Accountability	(Article 5) ■ Lawfulness, fairness, transparency ■ Purpose limitation ■ Data minimisation; accuracy ■ Storage limitation ■ Integrity & confidentiality ■ Accountability	(Section- 1798.100 - 1798.150) ■ Transparency ■ Accountability ■ Safeguarding of personal information ■ Prohibition of Discriminatory Practices

PrivacyPillar

Privacy Cheat Sheet

Topic	DPDPA & Draft Rules	GDPR	CCPA
Individual Rights	(Section 11-14) ■ Right to access ■ Right to correction and erasure ■ Right to grievance redressal ■ Right to nominate	(Article 12-22) ■ Right to access ■ Right to information ■ Right to Rectification ■ Right to erasure ■ Right to restrict processing ■ Right to object ■ Right to data portability ■ Rights related to automated decision making	(Section- 1798.100- 1798.150) ■ Right to deletion of personal information ■ Right to correct inaccurate personal information ■ Right to know ■ Right to limit use and disclosure of sensitive personal information ■ Right to no retaliation ■ Right of direct action
Obligations of Data Fiduciary/ Controller	■ Obtain valid consent ■ Implement security measures ■ Data Accuracy and Consistency ■ Notify data principals in case of breach ■ Publish contact details of representative or a DPO ■ Data Erasure	■ Determine the Purpose and Means of Processing (Article 24) Compliance with GDPR Principles (Article 5) ■ Respond to data subject rights. (Article 12-22) ■ Maintain Records of Processing Activities (Article 30) ■ Conduct Data Protection Impact Assessments (Article 35) ■ Data breach notification to relevant supervisory authority and affected data subjects (Article 33 &34) ■ Contractual Obligations with Processor (Article 28) ■ Cooperation with Supervisory Authorities (Article 31)	■ Privacy Notice Disclosure Honour opt-out requests ■ Consumer Information (Section-1798.100) :Inform consumers at collection about personal/sensitive data, purposes, and retention periods ■ Proportional Processing (Section-1798.130): Ensure data processing aligns with its purpose and original context ■ Agreements (Section-1798.100(d)) : Establish contracts ensuring limited disclosure, privacy compliance, and response to misuse ■ Data Security (Section-1798.100(e)): Implement safeguards against unauthorised access, destruction, or disclosure ■ Data Breach (Section-1798.150(a)): Notify consumers of any data breach expediently without delay
Obligations of Significant Data Fiduciary	(Section 10) ■ Appoint Data Protection Officer (DPO) ■ Appoint a data auditor and periodic audits ■ Conduct Data Protection Impact Assessment (DPIA)		
Data Breach Notification	DPDP Draft Rule 7 Notify affected Data Principals and the Board immediately after a data breach, including details, risks, and mitigation steps. Provide a detailed report to the Board within 72 hours.	(Article 33&34) Not all breaches need to be reported. If the breach is low risk: No reporting is required. If medium or high risk: Notify Supervisory Authority within 72 hours. If high risk: Notify affected data subjects in addition to the Supervisory Authority.	(Section- 1798.150(a)) Notify consumers when breaches affect personal information without any delay.

PrivacyPillar

Privacy Cheat Sheet

Topic	DPDPA & Draft Rules	GDPR	CCPA
Data Transfer	Subject to government restrictions and additional requirements as maybe notified by the government	Allowed only to countries with adequate protection or with safeguards in place	Not specifically restricted
Penalties	The data fiduciaries may be fined up to INR 250 crore per violation type ((with cumulative penalties possibly running into several hundred crores depending on breaches),while data principals can face penalties up to INR 10,000 for failing to observe their duties.	Penalties for non-compliance can be significant, with fines reaching up to €20 million or 4% of the company's total annual worldwide turnover, whichever is higher.	Consumers may sue for damages ranging from $100 to $750 per incident or for actual damages, may seek injunctive relief, and violations can result in fines of $2,500 per violation or $7,500 for intentional violations or those involving consumers under 16.